UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/818,567	03/28/2001	Soichi Furuya	520.39632VX1	4795

20457 7590 09/09/2004

ANTONELLI, TERRY, STOUT & KRAUS, LLP
1300 NORTH SEVENTEENTH STREET
SUITE 1800
ARLINGTON, VA 22209-9889

EXAMINER	
TRAN, ELLEN C	

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 09/09/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/818,567	FURUYA ET AL.	
	Examiner	Art Unit	
	Ellen C Tran	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 March 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *9-12,21-24 and 33-36* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *9-12,21-24 and 33-36* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

NORMAN M. WRIGHT
PRIMARY EXAMINER

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *2/4/04*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This action is responsive to communication: original application filed 08 March 2001, with acknowledgement of continuing application date from 16 February 2001, with acknowledgement of foreign application date of 09 March 2000.

2. Acknowledgement of Pre-Amendment filed 28 March 2001, claims 1-8, 13-20, 25-32, and 37 are withdrawn.

3. Claims 9-12, 21-24, and 33-36 are currently pending in this application. Claims 9, 21, and 33 are independent claims.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. **Claims 9 and 10** are rejected under 35 U.S.C. 103(a) as being unpatentable over Coppersmith et al. U.S. Patent No. 6,189,095 (hereinafter '095) in further view of Djakovic U.S. Patent No. 6,351,539 (hereinafter '539).

As to independent claim 9, "A symmetric-key decryption method comprising the steps of: dividing ciphertext to generate a plurality of ciphertext blocks each having a predetermined length" in '095 col. 5, lines 52-67 "A further object of the

present invention is to provide a technique whereby the cipher uses a variable number of stages (and therefore rounds) of processing during encryption"

"performing a decryption operation using said one of the plurality of ciphertext blocks, said random number block, and a feedback value obtained as a result of operation on still another one of the plurality of ciphertext blocks to produce a plaintext block" is shown in '539 col. 5, lines 40-51 "Still another object of the present invention is to provide a technique whereby the cipher used for encryption and decryption uses multiple stages, where each stage uses multiple Feistel network types that affect each word of the block"

the following is not taught in '095 however '539 teaches:

"generating a random number sequence based on a secret key; generating a random number block corresponding to one of said plurality of ciphertext blocks from said random number sequence" is shown in '539, col. 2, lines 19-26 "In one aspect, this invention is an encryption device which has a random number generator and three block cipher mechanisms ... An exclusive-or mechanism takes as input the first enciphered output from the first block cipher and output of the random number generator and produces a combined output";

"outputting a feedback value obtained as a result of operation on said one of the plurality of ciphertext blocks and said random number block, said feedback value being fed back to another one of the plurality of ciphertext blocks" is disclosed in '539 col. 2, lines 26-36 "The second block cipher mechanism takes as input the output of the exclusive-or mechanism and produces a second enciphered output based on the output of exclusive-or mechanism and on a second key";

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of '095 that shows a symmetric block cipher that uses multiple stages to include a random number generator. One of ordinary skill in the art would have been motivated to perform such a modification to strengthen the encryption algorithms used. As indicated by '539 (see col. 1, lines 48 et seq.) "One other known way to combine multiple blocks is to use two algorithms (and two independent keys). Using this approach, ... The ciphertext is the combined result of the two encryptions and is at least as strong as the stronger of the two encryption algorithms".

As to dependent claim 10, "wherein said decryption operation uses one or more said random number blocks whose total length is longer than a length of said one of the plurality of ciphertext blocks" is taught in '539, col. 2, lines 50-52 "The effective key length is the sum of key lengths used in BC1 and BC2 (256 in the preferred scheme)".

6. **Claims 11 and 12** are rejected under 35 U.S.C. 103(a) as being unpatentable over Coppersmith et al. U.S. Patent No. 6,189,095 (hereinafter '095) in further view of Djakovic U.S. Patent No. 6,351,539 (hereinafter '539) in further view of Wasilewski et al. U.S. Patent No. 6,424,714 (hereinafter '714).

As to dependent claim 11, "further comprising steps of: concatenating a plurality of said plaintext blocks to generate plaintext; extracting redundancy data included in said plaintext" is taught in '539 col. 4, lines 24-56 "That is, the DEMUX 28 extracts the enciphered random sequence SER from the input SC to the decryptor mechanism 26. The extracted sequence SER is deciphered using block cipher BC322-1

(in its decrypting mode) and the 256-bit key K3 to produce the random sequence SR. That is SR=BC3(SER, K3). The extracted sequence S3 is deciphered using block cipher BC220-1 (in its decrypting mode) using 128-bit key K2 to produce the sequence S2 which is then XORed (by XOR mechanism 24-1) with sequence SR to produce the sequence S1. That is, S1=SR.sym.BC2(S3, K2). Sequence S1 is deciphered using block cipher BC118-1 (in its decrypting mode), using 128-bit key K1, to produce the 64-bit plaintext. That is, the plaintext is produced by BC1(S1, K1)"

The following is not taught in the combination of teachings of '095 and '539 however '714 teaches:

"and checking said redundancy data to detect whether said ciphertext has been altered" in col. 4, lines 23-26 "and the second key, such that the STU can determine if the packets bearing the first key has been tampered with during transimssion".

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the combination teachings of '095 and '539 that show a symmetric block cipher that uses multiple stages with a random number generator to include detection of tampering with the decrypted data. One of ordinary skill in the art would have been motivated to perform such a modification because data transmitted over a digital network is more vulnerable to detection. As indicated by '714 (see col. 2, lines 28 et seq.) "In Lee, a program is scrambled at a SP site using a frequently changing random number. The random numbers are encrypted with a key and broadcast along with the program to customer sites. Customers who have paid receive the key, encrypted with the unique ID that is embedded in their set top unit (STU). These customers' STUs

can decrypt the key using the unique ID embedded therein. The customers' STU can then decrypt the encrypted random numbers, as they are broadcast, and use the random numbers, along with the key, to decrypt the program. As noted above, the key in the Lee invention must be securely transmitted; otherwise, an unauthorized user could get access to the key and gain access to the broadcast programs. Lee protects the key by using the unique ID of the STU to encrypt it. Such a technique works fine in a broadcast environment where there is a single broadcaster to multiple users. In that environment, the broadcaster can take adequate measures to protect the list of valid customer STU Ids ... However, in a digital network environment where STUs are uniquely addressable, and multiple SPs have access to multiple STUs, an unauthorized user could put information on the network addressed to individual STUs and thereby compromise the system. Applicants have recognized that a conditional access system in a digital network environment must have a mechanism that allows the STU to authenticate the identity of the SP. Thus, applicants have recognized that an improved encryption technique is needed".

As to dependent claim 12, "further comprising steps of: extracting secret data included in said plaintext; and checking said redundancy data and said secret data to detect whether said ciphertext has been altered" is taught in '714 col. 9, lines 55-65 "the STU 90, the MAC process is reversed before releasing the control word for use in decryption. The encrypted control word is parsed from the ECM and decrypted with the MSK (box 1008), which was transmitted to the STU 90 (as indicated by dashed lines in FIG. 3A) through a mechanism described in detail below. The now clear control word and the MSK are concatenated and hashed (box 1010) in similar fashion to the

technique used in the SABER 20 prior to transmission. This hash value is then compared to the MAC received in the ECM (1012). If the two values match then the control words are authorized for use by the STU 90 in decrypting the program" (it is inherent if the data was altered the STU would not be able to decrypt the program).

7. **Claims 21 and 22** are rejected under 35 U.S.C. 103(a) as being unpatentable over Coppersmith et al. U.S. Patent No. 6,189,095 (hereinafter '095) in further view of Djakovic U.S. Patent No. 6,351,539 (hereinafter '539).

As to independent claim 21, "A symmetric-key decryption apparatus comprising: a circuit for receiving ciphertext, and dividing the received ciphertext to generate a plurality of ciphertext blocks each having a predetermined length" in '095 col. 5, lines 52-67 "A further object of the present invention is to provide a technique whereby the cipher uses a variable number of stages (and therefore rounds) of processing during encryption"

"and a decryption operation circuit for performing a decryption operation using said one of the plurality of ciphertext blocks, said random number block, and a feedback value obtained as a result of operation on still another one of the plurality of ciphertext blocks to produce a plaintext block" is shown in '539 col. 5, lines 40-51 "Still another object of the present invention is to provide a technique whereby the cipher used for encryption and decryption uses multiple stages, where each stage uses multiple Feistel network types that affect each word of the block"
the following is not taught in '095 however '539 teaches:

"a circuit for receiving a secret key to generate a random number sequence whose length is longer than a length of said ciphertext, and generating a random number block corresponding to one of said plurality of ciphertext blocks from said random number sequence" is shown in '539, col. 2, lines 19-26 "In one aspect, this invention is an encryption device which has a random number generator and three block cipher mechanisms ... An exclusive-or mechanism takes as input the first enciphered output from the first block cipher and output of the random number generator and produces a combined output";

"a circuit for outputting a feedback value obtained as a result of operation on said one of the plurality of ciphertext blocks and said random number block, said feedback value being fed back to another one of the plurality of ciphertext blocks" is disclosed in '539 col. 2, lines 26-36 "The second block cipher mechanism takes as input the output of the exclusive-or mechanism and produces a second enciphered output based on the output of exclusive-or mechanism and on a second key";

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of '095 that shows a symmetric block cipher that uses multiple stages to include a random number generator. One of ordinary skill in the art would have been motivated to perform such a modification to strengthen the encryption algorithms used. As indicated by '539 (see col. 1, lines 48 et seq.) "One other known way to combine multiple blocks is to use two algorithms (and two independent keys). Using this approach, ... The ciphertext is the combined result of the two encryptions and is at least as strong as the stronger of the two encryption algorithms".

As to dependent claim 22, "wherein said decryption operation circuit uses one or more said random number blocks whose total length is longer than a length of said one of the plurality of ciphertext blocks" is taught in '539, col. 2, lines 50-52 "The effective key length is the sum of key lengths used in BC1 and BC2 (256 in the preferred scheme)".

8. **Claims 23 and 24** are rejected under 35 U.S.C. 103(a) as being unpatentable over Coppersmith et al. U.S. Patent No. 6,189,095 (hereinafter '095) in further view of Djakovic U.S. Patent No. 6,351,539 (hereinafter '539) in further view of Wasilewski et al. U.S. Patent No. 6,424,714 (hereinafter '714).

As to dependent claim 23, "further comprising: a circuit for concatenating a plurality of said plaintext blocks to generate plaintext; a circuit for extracting redundancy data included in said plaintext;" is taught in '539 col. 4, lines 24-56 "That is, the DEMUX 28 extracts the enciphered random sequence SER from the input SC to the decryptor mechanism 26. The extracted sequence SER is deciphered using block cipher BC322-1 (in its decrypting mode) and the 256-bit key K3 to produce the random sequence SR. That is SR=BC3(SER, K3). The extracted sequence S3 is deciphered using block cipher

BC220-1 (in its decrypting mode) using 128-bit key K2 to produce the sequence S2 which is then XORed (by XOR mechanism 24-1) with sequence SR to produce the sequence S1. That is, S1=SR.sym.BC2(S3, K2). Sequence S1 is deciphered using block cipher BC118-1 (in its decrypting mode), using 128-bit key K1, to produce the 64-bit plaintext. That is, the plaintext is produced by BC1(S1, K1)"

The following is not taught in the combination of teachings of '095 and '539 however '714 teaches:

"and a circuit for checking said redundancy data to detect whether said ciphertext has been altered" in col. 4, lines 23-26 "and the second key, such that the STU can determine if the packets bearing the first key has been tampered with during transimssion".

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the combination teachings of '095 and '539 that show a symmetric block cipher that uses multiple stages with a random number generator to include detection of tampering with the decrypted data. One of ordinary skill in the art would have been motivated to perform such a modification because data transmitted over a digital network is more vulnerable to detection. As indicated by '714 (see col. 2, lines 28 et seq.) "In Lee, a program is scrambled at a SP site using a frequently changing random number. The random numbers are encrypted with a key and broadcast along with the program to customer sites. Customers who have paid receive the key, encrypted with the unique ID that is embedded in their set top unit (STU). These customers' STUs can decrypt the key using the unique ID embedded therein. The customers' STU can then decrypt the encrypted random numbers, as they are broadcast, and use the random numbers, along with the key, to decrypt the program. As noted above, the key in the Lee invention must be securely transmitted; otherwise, an unauthorized user could get access to the key and gain access to the broadcast programs. Lee protects the key by using the unique ID of the STU to encrypt it. Such a technique works fine in a broadcast environment where there is a single broadcaster to multiple users. In that environment,

the broadcaster can take adequate measures to protect the list of valid customer STU Ids ... However, in a digital network environment where STUs are uniquely addressable, and multiple SPs have access to multiple STUs, an unauthorized user could put information on the network addressed to individual STUs and thereby compromise the system. Applicants have recognized that a conditional access system in a digital network environment must have a mechanism that allows the STU to authenticate the identity of the SP. Thus, applicants have recognized that an improved encryption technique is needed".

As to dependent claim 24, "further comprising: a circuit for extracting secret data included in said plaintext, wherein said circuit for detecting whether said ciphertext has been altered checks said secret data and said redundancy data to detect whether said ciphertext has been altered" is taught in '714 col. 9, lines 55-65 "the STU 90, the MAC process is reversed before releasing the control word for use in decryption. The encrypted control word is parsed from the ECM and decrypted with the MSK (box 1008), which was transmitted to the STU 90 (as indicated by dashed lines in FIG. 3A) through a mechanism described in detail below. The now clear control word and the MSK are concatenated and hashed (box 1010) in similar fashion to the technique used in the SABER 20 prior to transmission. This hash value is then compared to the MAC received in the ECM (1012). If the two values match then the control words are authorized for use by the STU 90 in decrypting the program" (it is inherent if the data was altered the STU would not be able to decrypt the program).

9. **Claims 33 and 34** are rejected under 35 U.S.C. 103(a) as being unpatentable over Coppersmith et al. U.S. Patent No. 6,189,095 (hereinafter '095) in further view of Djakovic U.S. Patent No. 6,351,539 (hereinafter '539).

As to independent claim 33, "A medium storing a program for causing a computer to perform a symmetric-key decryption method, wherein said program is read into said computer, said symmetric-key decryption method comprising the steps of: receiving ciphertext, and dividing the received ciphertext to generate a plurality of ciphertext blocks each having a predetermined length" in '095 col. 5, lines 52-67 "A further object of the present invention is to provide a technique whereby the cipher uses a variable number of stages (and therefore rounds) of processing during encryption"

"and performing a decryption operation using said one of the plurality of ciphertext blocks, said random number block, and a feedback value obtained as a result of operation on still another one of the plurality of ciphertext blocks to produce a plaintext block" is shown in '539 col. 5, lines 40-51 "Still another object of the present invention is to provide a technique whereby the cipher used for encryption and decryption uses multiple stages, where each stage uses multiple Feistel network types that affect each word of the block"

the following is not taught in '095 however '539 teaches:

"receiving a secret key to generate a random number sequence whose length is longer than a length of said ciphertext, and generating a random number block corresponding to one of said plurality of ciphertext blocks from said random

number sequence" is shown in '539, col. 2, lines 19-26 "In one aspect, this invention is an encryption device which has a random number generator and three block cipher mechanisms ... An exclusive-or mechanism takes as input the first enciphered output from the first block cipher and output of the random number generator and produces a combined output";

"outputting a feedback value obtained as a result of operation on said one of the plurality of ciphertext blocks and said random number block, said feedback value being fed back to another one of the plurality of ciphertext blocks" is disclosed in '539 col. 2, lines 26-36 "The second block cipher mechanism takes as input the output of the exclusive-or mechanism and produces a second enciphered output based on the output of exclusive-or mechanism and on a second key";

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of '095 that shows a symmetric block cipher that uses multiple stages to include a random number generator. One of ordinary skill in the art would have been motivated to perform such a modification to strengthen the encryption algorithms used. As indicated by '539 (see col. 1, lines 48 et seq.) "One other known way to combine multiple blocks is to use two algorithms (and two independent keys). Using this approach, ... The ciphertext is the combined result of the two encryptions and is at least as strong as the stronger of the two encryption algorithms".

As to dependent claim 34, "wherein said decryption operation uses one or more said random number blocks whose total length is longer than a length of said one of the plurality of ciphertext blocks" is taught in '539, col. 2, lines 50-52 "The

effective key length is the sum of key lengths used in BC1 and BC2 (256 in the preferred scheme)".

10. **Claims 35 and 36** are rejected under 35 U.S.C. 103(a) as being unpatentable over Coppersmith et al. U.S. Patent No. 6,189,095 (hereinafter '095) in further view of Djakovic U.S. Patent No. 6,351,539 (hereinafter '539) in further view of Wasilewski et al. U.S. Patent No. 6,424,714 (hereinafter '714).

As to dependent claim 35, "wherein said symmetric-key decryption method further comprises steps of: concatenating a plurality of said plaintext blocks to generate plaintext; extracting redundancy data included in said plaintext" is taught in '539 col. 4, lines 24-56 "That is, the DEMUX 28 extracts the enciphered random sequence SER from the input SC to the decryptor mechanism 26. The extracted sequence SER is deciphered using block cipher BC322-1 (in its decrypting mode) and the 256-bit key K3 to produce the random sequence SR. That is SR=BC3(SER, K3). The extracted sequence S3 is deciphered using block cipher
BC220-1 (in its decrypting mode) using 128-bit key K2 to produce the sequence S2 which is then XORed (by XOR mechanism 24-1) with sequence SR to produce the sequence S1. That is, S1=SR.sym.BC2(S3, K2). Sequence S1 is deciphered using block cipher BC118-1 (in its decrypting mode), using 128-bit key K1, to produce the 64-bit plaintext. That is, the plaintext is produced by BC1(S1, K1)"
The following is not taught in the combination of teachings of '095 and '539 however '714 teaches:

"and checking said redundancy data to detect whether said ciphertext has been altered" in col. 4, lines 23-26 "and the second key, such that the STU can

determine if the packets bearing the first key has been tampered with during transimssion".

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the combination teachings of '095 and '539 that show a symmetric block cipher that uses multiple stages with a random number generator to include detection of tampering with the decrypted data. One of ordinary skill in the art would have been motivated to perform such a modification because data transmitted over a digital network is more vulnerable to detection. As indicated by '714 (see col. 2, lines 28 et seq.) "In Lee, a program is scrambled at a SP site using a frequently changing random number. The random numbers are encrypted with a key and broadcast along with the program to customer sites. Customers who have paid receive the key, encrypted with the unique ID that is embedded in their set top unit (STU). These customers' STUs can decrypt the key using the unique ID embedded therein. The customers' STU can then decrypt the encrypted random numbers, as they are broadcast, and use the random numbers, along with the key, to decrypt the program. As noted above, the key in the Lee invention must be securely transmitted; otherwise, an unauthorized user could get access to the key and gain access to the broadcast programs. Lee protects the key by using the unique ID of the STU to encrypt it. Such a technique works fine in a broadcast environment where there is a single broadcaster to multiple users. In that environment, the broadcaster can take adequate measures to protect the list of valid customer STU Ids ... However, in a digital network environment where STUs are uniquely addressable, and multiple SPs have access to multiple STUs, an unauthorized user could put information on the network addressed to individual STUs and thereby compromise the system.

Applicants have recognized that a conditional access system in a digital network environment must have a mechanism that allows the STU to authenticate the identity of the SP. Thus, applicants have recognized that an improved encryption technique is needed".

As to dependent claim 36, "wherein said symmetric-key decryption method further comprises steps of: extracting secret data included in said plaintext; and checking said redundancy data and said secret data to detect whether said ciphertext has been altered" is taught in '714 col. 9, lines 55-65 "the STU 90, the MAC process is reversed before releasing the control word for use in decryption. The encrypted control word is parsed from the ECM and decrypted with the MSK (box 1008), which was transmitted to the STU 90 (as indicated by dashed lines in FIG. 3A) through a mechanism described in detail below. The now clear control word and the MSK are concatenated and hashed (box 1010) in similar fashion to the technique used in the SABER 20 prior to transmission. This hash value is then compared to the MAC received in the ECM (1012). If the two values match then the control words are authorized for use by the STU 90 in decrypting the program" (it is inherent if the data was altered the STU would not be able to decrypt the program).

Conclusion

11. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ellen C Tran whose telephone number is (703) 305-8917. "**After 26 October 2004, the examiner can be reach at (571) 272-3842".** The examiner can normally be reached on 6:30 am to 3:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A Morse can be reached on (703) 308-4789. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

NORMAN M. WRIGHT
PRIMARY EXAMINER

Ellen Tran
Patent Examiner
Technology Center 2134
3 September 2004